



ROBERT M. MORGENTHAU
DISTRICT ATTORNEY

DISTRICT ATTORNEY
OF THE
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N. Y. 10013
(212) 335-9000

January 19, 2007

Attorney General Alberto R. Gonzales
Chairman Deborah Platt Majoras
President's Identity Theft Task Force
Federal Trade Commission/Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.
Washington D.C. 20580

Re: **Identity Theft Task Force**

Dear Attorney General Gonzales and Chairman Majoras:

In November 2004, in recognition of the growing threat posed by identity theft nationwide, I created a unit within my office dedicated solely to the investigation and prosecution of this form of crime. Believed to be the first and largest of its kind, the Identity Theft Unit was established in response to the marked rise in complaints from individual and corporate victims in our jurisdiction, as well as to the growing sophistication of the criminals perpetrating these crimes. There are currently over seventy Assistant District Attorneys actively engaged in identity theft prosecutions in my Office. The cases they investigate include everything from simple credit card theft to complex international criminal rings engaged in the highest levels of fraud.

I commend the President's Identity Theft Task Force for identifying many of the critical issues requiring urgent attention from both the public and private sectors if identity theft is to be stopped. Based on my unit's experience in handling over 5,700 identity-theft-related cases, I could provide remarks on virtually every subject raised in the Task Force's Summary of Issues. However, for the purpose of this response, I will limit my comments to a few of the specific areas highlighted in the Summary.

I. Encouraging State Prosecutions

In its Summary of Issues, the Task Force queries whether encouraging state prosecutions of identity theft would meaningfully assist in increasing the number of

identity theft prosecutions (IV(4), "Prosecutions of Identity Theft"). I hope that a significant outcome of the Identity Theft Task Force's work will be to recognize the vital role that state and local prosecutors play in the fight against identity theft. Any measures designed to assist local prosecutors' offices in handling the bulk of the country's identity theft caseload would increase the number of identity theft prosecutions undertaken nationwide.

Local prosecutors are well positioned to detect trends, identify criminal organizations and launch significant investigations. Identity theft cases prosecuted at the local level frequently begin with a summary arrest of a defendant caught in the act of identity theft, or through follow-up investigation from an identity theft victim's complaint to his local police department. While many of these cases require relatively little investigation for a successful prosecution, many other cases are identified early on as "the tip of the iceberg." In such instances, the investigation of the complaint of one citizen, or the arrest of one individual, leads to the exposure of a major data breach or the discovery of an organized identity theft ring perpetrating a multifaceted series of crimes. Thus, in processing summary arrests and responding to identity theft complaints, state-level investigators and prosecutors can end up launching large-scale investigations using sophisticated techniques such as wiretaps, informants, undercover operations, and internet stings.

For these reasons, Assistant District Attorneys in our Identity Theft Unit have conducted numerous investigations and prosecutions of the most complex kind. For example, we have prosecuted cases arising from major corporate or public sector data breaches with hundreds or thousands of victims, large rings of credit card and check counterfeiters, individuals and groups engaged in local and international identity-theft-related cybercrime, and conspiracies to steal and use personal identifying information throughout our region and the country. We often collaborate with other local prosecutors' offices - such as the Hudson County Prosecutor's Office in Jersey City, New Jersey - to effectively dismantle a criminal organization.

My Office concentrates on these organized criminal groups because rooting out those who treat crime as a business can eliminate entire hubs of identity theft activity. Simultaneously, however, our Assistant District Attorneys continue to handle the hundreds of routine identity theft arrests that are made in Manhattan every year. Almost every day in this borough, police officers arrest an average of five or six people for felony crimes involving identity theft. These individuals are arrested for stealing credit cards or using stolen credit cards, shopping with counterfeit credit cards, cashing counterfeit checks, possessing forged identification documents for the purpose of defrauding the police, banks or merchants, or using stolen personal identifying information in a myriad of other ways.

Investigating and prosecuting this burgeoning wave of identity theft requires a substantial investment of resources. While these cases are coming into my office at a rate akin to certain everyday street crimes, the techniques required to prosecute them properly are those more typically associated with long-term white collar investigations. This

combination of a mushrooming intake with the time-consuming investigative methods needed to solve these crimes can hinder local prosecutors' offices from pursuing each case to the extent it deserves.

I have made the decision to devote substantial resources to identity theft prosecutions. Currently, the unit here is staffed by two unit chiefs, seven prosecutors specially assigned to long-term investigations, 65 prosecutors assigned to prosecute typical identity theft cases, four investigative analysts and a computer forensic examiner/investigator. When local prosecutors and law enforcement do not have the funds or personnel for such a comprehensive, intensive approach to the problem, there is generally no other prosecutorial agency to do the work. The result is that crimes go undetected and criminal organizations function with impunity.

It is important to note that, in contrast to many other crimes, it is not unusual for a local prosecutor to handle an identity theft case investigated by a federal law enforcement agency. Understandably, United States Attorney's Offices do not prosecute identity theft cases unless they meet certain threshold requirements. Indeed, if these offices did not create these thresholds, they would be overrun by the volume of identity theft cases within their locales. As a result, some cases are referred to local prosecutors' offices after being declined by federal prosecutors, and such cases are often the type of "tip of the iceberg" cases which lead to long-term investigations described above.

Unfortunately, these referrals for local prosecution are not occurring as frequently as they should. As we understand it, most federal law enforcement agencies do not have structural mechanisms for referring cases for local prosecution. In some instances, federal law enforcement agencies indicate that they are mandated to bring all cases or investigative leads to United States Attorney's Offices - despite the fact that these offices regularly decline to act. Thus, a federal law enforcement agency can successfully uncover the existence of an organized criminal group, present the case to a United States Attorney's Office, have that office decline to prosecute, and then have no avenue to bring these criminals to justice. The lack of institutional incentives for state-level prosecutions serves as a major hindrance in law enforcement's fight against the identity theft epidemic.

I am happy to report that despite the current incentive structure, we are in the midst of several large-scale identity theft investigations in conjunction with the United States Secret Service and the United States Postal Inspection Service. We consider these agencies great allies in our collective mission to fight identity theft.

In short, since local prosecutors' offices are bearing the brunt of the identity theft caseload, measures to fund an increase in the number of local prosecutors, investigators, analysts, and computer forensic specialists dedicated to identity theft cases will improve the number of prosecutions nationwide. Creating protocols to encourage and enable federal law enforcement agencies to refer cases for state and local prosecution would also assist in increasing the overall number of identity theft prosecutions. And promoting national training initiatives to educate both state and federal prosecutors about the relevant legal, technological, and investigative issues can only benefit us all.

II. Measuring Law Enforcement's Efforts

The Identity Theft Task Force has correctly observed that there is little data available evaluating law enforcement's response to identity theft. In order to improve our Office's methods in this area, our unit has tracked statistics on identity-theft-related cases prosecuted in Manhattan since November 1, 2004. The data include details of the individual defendants and victims, the classification of identity theft crimes committed, and the results of our prosecutorial efforts as reflected in the disposition of the cases and sentences imposed. To date, we have collected data on over 5,700 cases.

Given that the Task Force is contemplating a National Identity Theft Enforcement Center tasked with centralizing intelligence about identity theft, we note the powerful effect such a database has had in centralizing this information within our jurisdiction. One of our primary uses of this database is to determine whether connections exist between ongoing prosecutions. For example, two people might be arrested separately in different locations using the same victim's personal information, or the same type of forged credit card, or conducting an identity theft crime using the same signature method. Before we began tracking case data, multiple investigators and prosecutors were simultaneously working on different pieces of the same criminal puzzle without coordination. By capturing the details of cases in our database, we are now often able to detect patterns or links between crimes at an early stage of the investigation. Thus, the database has become an invaluable resource in focusing our investigations as effectively as possible.

Moreover, one of the challenges to prosecuting this type of criminal activity is that identity thieves frequently conduct their criminal activity in multiple jurisdictions. Assistant District Attorneys in the Identity Theft Unit regularly find themselves reaching out to victims, corporations and law enforcement agencies in cities and states across the country in order to investigate crimes perpetrated here in Manhattan. Not infrequently, they discover that the targets or the activity they are scrutinizing have raised suspicion elsewhere. A database or national repository through which investigators could share intelligence about identity theft on a national basis could be a tremendous resource.

I would also encourage the Task Force to pursue measures that would require financial institutions to contribute reports of fraud to such a database. In our experience, many identity theft victims report crimes to their banks and credit card companies, but fail to alert law enforcement. Thus, adding fraud data collected by financial institutions to the proposed national database would considerably improve the breadth of the intelligence and analysis it can provide.

III. Identity Thieves in Foreign Countries

One of the primary impediments to the prosecution of identity theft is the ability of prolific cybercriminals to hide behind computers in foreign countries. If successful, the steps outlined by the Identity Theft Task Force to encourage international cooperation in fighting cybercrime could well assist United States law enforcement in bringing many identity thieves to justice.

In addition to asking for assistance from foreign governments, however, we could do more within the United States to limit the reach of foreign identity thieves by denying them fraudulent access to our financial and telecommunications systems. Sadly, many foreign cybercriminals victimize our individual and corporate citizens by taking advantage of resources which, though available globally, are controlled domestically.

For example, my Office initiated a prosecution last year against Western Express International, Inc. and its principals - Vadim Vassilenko and Yelena Barysheva. We determined that these defendants, operating out of a small office in midtown Manhattan, were providing anonymous financial services to hundreds of customers in Eastern Europe and Russia. In violating our state's banking regulations prohibiting unauthorized money transmitting and check cashing, the defendants utilized the services of domestic banks, credit card companies, money remitting services, and internet service providers to move over 25 million dollars overseas. Moreover, the defendants' used anonymous digital currencies, such as Egold and Webmoney, as some of their primary methods of unlawfully transmitting funds. The practices of these "virtual currency" systems are entirely unregulated by our federal or state banking agencies. Considering the fact that many of Western Express' customers were cybercriminals known to victimize American consumers, the danger of such a company operating within our country is readily apparent.

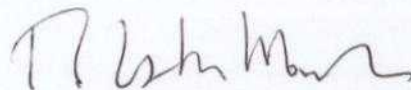
Our experience with the Western Express investigation indicates that there are steps that can be taken locally and nationally to prevent this type of criminal hub from developing. First, our financial institutions must be encouraged to aggressively identify accounts being used for illegal purposes. In the Western Express case, accounts used to wire millions of dollars overseas went undetected by banks for long periods of time. National money remittal systems were also improperly utilized to wire money abroad. Second, anonymous financial services such as Egold and Webmoney must be regulated if they are to do business in the United States. The existence of such systems, which allow money to be moved anonymously around the world, significantly increases the ability of criminals to launder identity theft proceeds earned in this country. And third, federal and local law enforcement must be vigilant in determining whether such entities have opened for business within their jurisdictions. In the case of Western Express, other law enforcement agencies had identified suspicious financial activity emanating from the company. However, steps were not taken to prosecute the entity until an Assistant District Attorney in my Office stumbled on Western Express in the course of a routine stolen credit card investigation. The lesson learned is that, left unchecked, outfits like Western Express will continue to form and prosper right under our noses.

We continue to investigate the money laundering activities of Western Express, as well as many other cases involving foreign criminals using the internet to commit identity theft crimes in the United States. In almost every cyber case, identity thieves make use of the services of our domestic internet service providers to commit their crimes. Spyware, malware, phishing, pharming, botnets, proxying of internet protocol addresses - all rely in some way on the internet services that American companies provide. Many internet service providers and internet businesses actively work to prevent the fraudulent use of their products. If the President's Identity Theft Task Force could promote these practices among all companies, and encourage the investment in technology needed to stop criminal misuse of the internet, foreign criminals might someday be prevented from committing these crimes from afar.

It is our belief that while prosecutors in the United States, at times, may not be able to pursue foreign targets, our financial and telecommunications industries should not allow themselves to be unwitting participants in these criminal activities. The Identity Theft Task Force could take steps to encourage domestic institutions to develop the technology and practices needed to prevent foreign criminals from using our networks to commit identity theft.

I thank you and the Identity Theft Task Force for allowing me the opportunity to comment on its proposals. It is gratifying to find that you are addressing so many of the issues we confront in our daily fight against identity theft. If my office can be of any assistance to the Identity Theft Task Force and its working groups in implementing its recommendations, please do not hesitate to contact me.

Sincerely,

A handwritten signature in dark ink, appearing to read "R. M. Morgenthau", with a stylized, flowing script.

Robert M. Morgenthau